

Cámara de Representantes

XLVIII Legislatura

DIVISIÓN PROCESADORA DE DOCUMENTOS

Nº 243 de 2015

Carpetas Nos. 2882, 2949, 3002, 3003, 3012 de 2014 y 3035 de 2015

Comisión de Asuntos Internacionales

SEÑOR SUBSECRETARIO DEL MINISTERIO DE DEFENSA NACIONAL,
DOCTOR JORGE MENÉNDEZ

"La Ciberguerra"

ACUERDO CON EL REINO DE LOS PAÍSES BAJOS SOBRE INTERCAMBIO DE INFORMACIÓN TRIBUTARIA Y SU PROTOCOLO Y NOTAS REVERSALES

ACUERDO MARCO DE COMERCIO E INVERSIÓN CON EL GOBIERNO DE LA REPÚBLICA SOCIALISTA DE VIETNAM

ACUERDO SOBRE COOPERACIÓN ECONÓMICA CON LA REPÚBLICA DE ARMENIA

ACUERDO DE COOPERACIÓN EN MATERIA DE DEPORTES CON EL GOBIERNO DE LA REPÚBLICA DE ARMENIA

ACUERDO CON EL GOBIERNO DE LA REPÚBLICA SOCIALISTA DE VIETNAM PARA EVITAR LA DOBLE IMPOSICIÓN Y PREVENIR LA EVASIÓN FISCAL EN MATERIA DE IMPUESTOS SOBRE LA RENTA Y SOBRE EL PATRIMONIO

ACUERDO CON LA REPÚBLICA DEL PERÚ SOBRE COOPERACIÓN EN ASUNTOS MIGRATORIOS

Versión taquigráfica de la reunión realizada
el día 9 de setiembre de 2015

(Sin corregir)

Preside:	Señor Representante Daniel Peña Fernández.
Miembros:	Señores Representantes Roberto Chiazzaro, Jorge Meroni, Silvio Ríos Ferreira y Tabaré Viera Duarte.
Delegados de Sector:	Señores Representantes Pablo González y José Carlos Mahía.
Invitados:	Señor Subsecretario del Ministerio de Defensa Nacional, doctor Jorge Menéndez; Capitán de Navío Roberto Ambrosoni, Jefe del Departamento de Sistemas de Información y el señor Claudio Alonso, Director de Asuntos Internacionales, Cooperación y Derecho Internacional.
Secretario:	Señor Gonzalo Legnani.
Prosecretario:	Señor Daniel Conde Montes de Oca.

═══════II═══════

SEÑOR PRESIDENTE (Daniel Peña Fernández).- Habiendo número, está abierta la reunión.

——Antes de invitar a pasar al señor Subsecretario de Defensa Nacional, para tratar el asunto relativo a su Cartera, propongo concluir el resto de los puntos.

Se pasa a considerar el segundo punto del orden del día: "Acuerdo con el Reino de los Países Bajos sobre intercambio de información tributaria y su protocolo; y notas reversales".

SEÑOR MERONI (Jorge).- Esto se enmarca en los acuerdos que Uruguay ha firmado, como surge del artículo 26 de la OCDE. Este acuerdo no tiene inconvenientes. Uruguay ya firmó convenios de información tributaria con Argentina, Australia, Brasil, Francia, Dinamarca, Noruega y Groenlandia.

Este proyecto se presentó en la Legislatura pasada y nosotros pedimos su desarchivo, por lo que aconsejamos que sea aprobado por esta Comisión.

SEÑOR VIERA DUARTE (Tabaré).- Es cierto que hay otros acuerdos de este tenor que se han aprobado en el Parlamento en la Legislatura pasada, pero también se han aprobado una cantidad de acuerdos de intercambio de información tributaria y de protección de inversiones. Este acuerdo no es de protección de inversiones. Al final de la Legislatura pasada, el Partido Colorado tomó la resolución de no votar los acuerdos que no contengan la protección de inversiones. Nos parece que un acuerdo solo de información tributaria queda rengo.

Por lo tanto, anuncio mi voto negativo.

SEÑOR PRESIDENTE.- Si no se hace uso de la palabra, se va a votar.

(Se vota)

——Cuatro en cinco: AFIRMATIVA.

Se pasa a considerar el tercer punto del orden del día: "Acuerdo marco de comercio e inversión con el Gobierno de la República Socialista de Vietnam".

SEÑOR MERONI (Jorge).- Este Acuerdo se basa en el reconocimiento que manifiestan ambos Estados en cuanto a la importancia de promover un ambiente abierto y previsible para el comercio internacional y la inversión. Asimismo, se destaca el deseo de reducir las barreras arancelarias, a fin de facilitar el ingreso a los mercados y el acuerdo preexistente entre ambos Estados para la protección y promoción de inversores, así como el deseo de asegurar que sus políticas comerciales y ambientales promuevan mutuamente el desarrollo sostenible.

Este proyecto fue presentado en la Legislatura pasada y pedimos su desarchivo, por lo que aconsejamos su aprobación.

SEÑOR PRESIDENTE.- Si no se hace uso de la palabra, se va a votar.

(Se vota)

——Cinco por la afirmativa: AFIRMATIVA. Unanimidad.

Se pasa a considerar el cuarto punto del orden del día: "Acuerdo sobre cooperación económica con la República de Armenia".

SEÑOR MERONI (Jorge).- Este Acuerdo es de cooperación económica con la República de Armenia. Creemos que debe ser aprobado. Se busca fomentar la realización de actividades que creen y profundicen los lazos económicos entre ambas

partes, contribuyendo a un adecuado clima de negocios. Desde hace muchos años, Uruguay tiene un vínculo muy estrecho con la República de Armenia.

Este proyecto se presentó en la Legislatura pasada y aconsejamos aprobarlo porque sirve para el desarrollo de la cooperación internacional entre Uruguay y la República de Armenia.

SEÑOR PRESIDENTE.- Si no se hace uso de la palabra, se va a votar.

(Se vota)

——Cinco por la afirmativa: AFIRMATIVA. Unanimidad.

Se pasa a considerar el quinto punto del orden del día: "Acuerdo de cooperación en materia de deportes con el Gobierno de la República de Armenia".

SEÑOR MERONI (Jorge).- La aprobación del presente acuerdo pondrá al servicio de las relaciones de ambos países un instrumento práctico y abierto que se ajustará a la necesidad de nuestro país de profundizar las relaciones de cooperación deportiva con Armenia, al aportar un marco jurídico que actuará como herramienta de trabajo, bajo la cual se podrá incrementar la relación bilateral en un área de interés para ambas partes. Para el cumplimiento del presente Acuerdo, las partes alentarán a sus federaciones, uniones, asociaciones e instituciones deportivas nacionales a establecer y desarrollar vínculos directos, así como a promover el intercambio de técnicos y delegaciones deportivas.

Este proyecto fue presentado en la Legislatura pasada y la Comisión pidió su desarchivo, por lo que aconsejamos su aprobación.

SEÑOR PRESIDENTE.- Si no se hace uso de la palabra, se va a votar.

(Se vota)

——Cinco por la afirmativa: AFIRMATIVA. Unanimidad.

Se pasa a considerar el sexto punto del orden del día: "Acuerdo con el Gobierno de la República Socialista de Vietnam para evitar la doble imposición y prevenir la evasión fiscal en materia de impuestos sobre la renta y sobre el patrimonio".

SEÑOR MERONI (Jorge).- Este Acuerdo con la República de Vietnam está basado en los problemas de doble tributación internacional que surgen cuando dos países se encuentran involucrados en el cobro del impuesto a un mismo sujeto. Los Estados, para enfrentar y resolver los casos de doble imposición internacional, celebran acuerdos o convenios para regular esta situación. Estos convenios no solo contemplan las reglas que usarán para evitar la doble imposición, sino también los mecanismos para que se dé la colaboración entre las administraciones tributarias, a fin de detectar casos de evasión fiscal. Mediante el uso del convenio, los Estados firmantes renuncian a gravar determinadas ganancias y acuerdan que sea solo uno de los Estados el que cobre el impuesto o, en todo caso, que se realice una imposición compartida entre ambos Estados.

Nuestro país adoptó estándares internacionales propuestos por OCDE, en el marco de convenios para evitar la doble imposición y, en esta materia, ha suscrito acuerdo con Alemania, Hungría, México, España, Portugal, Suiza, India, Malta, Finlandia, etcétera.

Asimismo, se establecen los métodos para evitar la doble tributación, los procesos para resolver controversias y los mecanismos de intercambio de información entre las autoridades competentes de los Estados contratantes.

Este proyecto también fue desarchivado por esta Comisión. Por lo tanto, aconsejamos su aprobación en el día de hoy.

SEÑOR PRESIDENTE.- Si no se hace uso de la palabra, se va a votar.

(Se vota)

——Cinco por la afirmativa: AFIRMATIVA. Unanimidad.

Se pasa a considerar el séptimo punto del orden del día: "Acuerdo con la República del Perú sobre cooperación en asuntos migratorios".

SEÑOR MERONI (Jorge).- Se destaca que el objetivo del presente Acuerdo es el establecimiento de mecanismos de cooperación entre las partes que permitan diseñar programas en las diversas áreas de migración -como en la laboral-, programas de interculturalidad y de combate a la trata de personas y mecanismos expeditados para la regularización de los migrantes. Se establece que las partes, de acuerdo con sus respectivos planes presupuestarios, asignarán el aporte que se efectuará para el desarrollo de las actividades contempladas en este Acuerdo, así como en lo que respecta a la participación de los funcionarios y de los profesionales de las instituciones públicas involucradas.

Por lo expuesto y siendo este un proyecto desarchivado en esta Legislatura, aconsejamos su aprobación en el día de hoy.

SEÑOR PRESIDENTE.- Si no se hace uso de la palabra, se va a votar.

(Se vota)

——Cinco por la afirmativa: AFIRMATIVA. Unanimidad.

Dese cuenta de los asuntos entrados.

SEÑOR SECRETARIO (LEGNANI, Gonzalo).- 1.- ACUERDO MARCO DE COOPERACIÓN CON LA REPÚBLICA COOPERATIVA DE GUYANA (C/449/15 Rep. 281/15). 2.- ACUERDO MARCO DE COOPERACIÓN CON LA REPÚBLICA DE SURINAM (C/450/15 Rep. 282/15). 3.- CONVENIO CON EMIRATOS ÁRABES UNIDOS PARA EVITAR LA DOBLE IMPOSICIÓNY PREVENIR LA EVASIÓN FISCAL EN MATERIA DE IMPUESTOS SOBRE LA RENTA Y SOBRE EL PATRIMONIO (C/452/15 Rep. 284/15). 4.- ACUERDO CON LA REPÚBLICA DE CHILE PARA EL INTERCAMBIO DE INFORMACIÓN EN MATERIA TRIBUTARIA (C/453/15 Rep. 285/15).

SEÑOR PRESIDENTE.- Adelanto que informaré el asunto de la Carpeta N° 452, ya que asistiré a ese país durante este mes.

(Ingresan a sala integrantes del Ministerio de Defensa Nacional)

——La Comisión da la bienvenida a una delegación del Ministerio de Defensa Nacional, integrada por el doctor Jorge Menéndez, Subsecretario, el capitán de navío Roberto Ambrosoni, jefe del Departamento de Sistemas de Información, y el señor Claudio Alonso, Director de Asuntos Internacionales, Cooperación y Derecho Internacional Humanitario.

Los hemos convocado a raíz de un planteo que ha hecho el señor diputado Mahía relativo a la *ciberguerra*.

Por otra parte, como este Parlamento creó una comisión de apoyo al papel de Uruguay como miembro no permanente del Consejo de Seguridad de Naciones Unidas, si quedara un poco de tiempo -a la hora 14 se reúne la Cámara-, nos gustaría que el señor

subsecretario nos diera un breve informe con respecto al papel de las misiones de paz. De lo contrario, coordinaremos una nueva reunión.

SEÑOR MAHÍA (José Carlos).- Agradezco a la comisión por tener en agenda este asunto.

Como ya hemos dicho, llevamos este tema -no en términos personales sino con el acuerdo de la bancada parlamentaria uruguaya- a uno de los tres organismos que suscribe el Parlamento Nacional, la Unión Interparlamentaria, para que lo analizara, ya que tiene múltiples abordajes y una actualidad cada vez mayor en el mundo. Desde ese punto de vista, entendimos que esta comisión del Cuerpo debía conocer los aspectos que presentamos en nombre de Uruguay.

La *ciberguerra* implica temas que hacen a la seguridad de los estados, a los derechos individuales de las personas y a dos pilares que parecen antagónicos frente a este nuevo fenómeno, sobre el que cada día se conocen mayores novedades: por un lado, la seguridad personal, privada y de los organismos de los Estados y, por otro lado, la libertad individual y el derecho a la privacidad. El hecho es que el mundo está transitando sobre esos dos pilares y aún no hay decisiones acordadas en materia internacional. En consecuencia, los poderes ejecutivos y los organismos multilaterales van a tener que avanzar para actualizar estas convenciones, que refieren en forma específica a proteger adecuadamente a los ciudadanos en el mundo, salvaguardando estos dos aspectos fundamentales.

Este asunto tiene una alta complejidad política y técnica, pero como es de mucha actualidad, quisimos tratarlo en los organismos internacionales y también en esta comisión.

Digo esto a modo de introducción. Los documentos están al alcance de todos.

SEÑOR SUBSECRETARIO DE DEFENSA NACIONAL.- Siempre es un gusto estar en esta Casa. Saludo a los funcionarios y a los diputados presentes en sala.

El tema planteado por el señor diputado Mahía interesa mucho al Ministerio de Defensa Nacional y al Gobierno.

Desde nuestra área de responsabilidad, pretendemos encararlo desde el punto de vista de la seguridad y de la seriedad necesarias. Debemos tener en cuenta que en relación a la defensa nuestro país tradicionalmente se manejó en tres terrenos: el aire, el mar y la tierra, con las respectivas fuerzas y los respectivos comandos allí desplegados.

Hoy, el mundo transita la experiencia de un nuevo escenario: el *ciberespacio*. Se trata de un escenario sin fronteras, en donde está Internet, los ordenadores, los sistemas y la vida virtual de todos los que estamos aquí presentes. Es un escenario globalizado, interdependiente, de relaciones al instante y de conocimientos lejanos al presente. Pero el avance de la tecnología ha traído, también, el desarrollo de cierto tipo de inseguridades.

Como decía, Internet no tiene fronteras; los límites no son los de los países. Esas fronteras, tan difusas y globales, han hecho que no existan respuestas claras y consecuentes con la profundidad de los problemas que los Estados tienen que tratar, tal vez porque este problema surgió hace poco tiempo.

Estoy de acuerdo con el señor diputado Mahía en que, teniendo en cuenta la magnitud del tema, las respuestas desde el punto de vista legal aún no están al día, no están *aggiornadas*, tanto a nivel internacional como nacional.

Este tema vino para quedarse. Sucintamente -porque sé que el tiempo que tienen hoy no es suficiente- voy a relatar tres hechos particulares que se dieron en el mundo.

En 2003, Estados Unidos tuvo un apagón generalizado, que luego se supo fue producto de un sabotaje a través de las redes.

En 2007, Estonia entró en conflicto con otro país y perdió la conexión a nivel internacional como país en su conjunto; previamente, la habían perdido los partidos políticos, las instituciones nacionales, los actores nacionales, los parlamentarios. Ese hecho marco un hito a nivel internacional en relación al tema que estamos tratando.

En el año 2010, se detectó la presencia del virus Stuxnet. Se trata de un virus específico, creado para sabotear procesos industriales en el área nuclear, que afectó a Irán. Pero esto no es como cuando se dispara un misil, que cae en determinado lugar y afecta esa zona; con esto se dispara hacia un lugar y los ordenadores y los sistemas repican este tipo de acciones hacia otros lugares y la destrucción es mucho mayor.

Estos tres problemas de carácter emblemático, además de otra inmensa cantidad de hechos -muchos sucedidos en Uruguay-, han generado conciencia sobre la necesidad de dar respuesta y de organizarse con respecto a esta nueva situación.

El Ministerio de Defensa Nacional, en línea con lo que el Gobierno nacional ha determinado a través de decretos y de resoluciones, desde hace ya algún tiempo ha actuado, pero no de manera demasiado pública. A veces, la actuación del Ministerio de Defensa Nacional va acompañada por la reserva correspondiente al área en la que nos toca actuar. Lo cierto es que algo hemos hecho, y eso es lo que queremos mostrarles.

Tenemos alguna diferencia en cuanto a la catalogación de determinado tipo de hechos.

Nosotros somos un país de paz. Pretendemos, y en ese sentido hemos trabajado con ahínco en los organismos que integramos -fundamentalmente a nivel regional-, que este sea un continente de paz. Por tanto, la conceptualización de las dificultades que tenemos tiene que ver con ese concepto, con mirar el mundo desde la paz.

No vemos los *ciberataques* de carácter personal, corporativo, grupal o de Estado como una situación de guerra. Por lo tanto, analizamos la *ciberguerra* desde el punto de vista de la defensa y la conceptualización es como *ciberdefensa*.

Para nosotros la *ciberseguridad* es el conjunto de acciones y medidas activas y pasivas de carácter preventivo, proactivo y reactivo, tomadas en el contexto de las redes y sistemas informáticos, para la preservación de la disponibilidad, integridad y confidencialidad de la información, sistemas de información e infraestructuras de comunicaciones asociadas.

Asimismo, consideramos que la *ciberdefensa* es el conjunto de acciones y medidas activas y pasivas de carácter preventivo, proactivo y reactivo, tomadas en el contexto de las redes y de los sistemas informáticos con el objetivo de asegurar la correcta operación de la infraestructura de sistemas informáticos en el ámbito de la defensa nacional, de acuerdo a las políticas y reglamentaciones vigentes.

Por otra parte, nuestro cometido es asegurar el correcto funcionamiento de las infraestructuras informáticas y su interacción con el *ciberespacio* acorde a las políticas y reglamentaciones vigentes, con el propósito de permitir el cumplimiento de todas las actividades y cometidos en el ámbito de la defensa nacional.

Cuando hablamos del ámbito de defensa nacional nos remitimos a la definición de defensa nacional aprobada unánimemente por este Parlamento, en la Ley Nº18.650 de

2010. No solamente entiende aspectos militares, sino también los que tienen que ver con la soberanía, con la integridad territorial, con la defensa de nuestros activos críticos, con el bienestar presente y futuro de la población.

Asimismo, se debe garantizar la disponibilidad, integridad y confidencialidad de la información y de las infraestructuras de las redes informáticas en el área de la defensa. Se deben estudiar e implementar medidas y *contramedidas* acordes con la función y la información recabada y asociada a incidentes, *ciberataques,* riesgos y vulnerabilidades en el ámbito de la defensa nacional. Para nosotros es práctica normal y más eficiente el contar con equipos de respuesta específicos -que tenemos en el Ministerio- en el campo de aplicación específica. Ese es uno de los conceptos que nosotros manejamos. Para nuestro país es bueno contar en defensa con un centro de respuesta como el Dcsirt, creado a partir del Decreto 36 del año 2015.

Tenemos una estructura formada de acuerdo con un esquema del que les dejo una copia para que puedan verlo. Es necesario que los equipos de respuesta sean únicos en su especialidad, pero que colaboren entre ellos.

SEÑOR PRESIDENTE.- ¿Hay comunicación con Agesic?

SEÑOR SUBSECRETARIO DE DEFENSA NACIONAL.- Sí; más adelante voy a informar al respecto.

Ahora me voy a referir a la forma en que funcionamos y a los antecedentes de *ciberseguridad* en el Ministerio de Defensa Nacional. En el Ministerio se encuentra el punto físico de contacto nacional del Comité Interamericano contra el Terrorismo. Es el Subsecretario de Defensa, de acuerdo con la Resolución 1519 del año 2001, hasta el presente.

Desde hace años, el Ministerio de Defensa Nacional forma parte de la Red Hemisférica Sur de puntos de contacto de seguridad cibernética del CICTE, colaborando en cursos de capacitación, siendo coorganizador de eventos de seguridad y asistiendo a otros integrantes de la red en caso de incidentes cibernéticos.

En la órbita del Ministerio de Defensa Nacional se encuentran gran cantidad de activos críticos -luego los mencionaré-, cuyo funcionamiento depende directamente de los sistemas de información que tiene asociados; activos críticos del Ministerio y del Estado.

En el Ministerio de Defensa Nacional existen además de los activos críticos típicos de cualquier organización basada en sistemas de información para su funcionamiento, otros de características específicas cuyo descuido puede ocasionar graves incidentes.

El Ministerio de Defensa Nacional está llevando a cabo la gestión de la seguridad de la información en el Inciso de la siguiente forma: cumplió con el Decreto 452/009, teniendo un responsable de de seguridad en el Inciso, que es el Capitán de Navío Roberto Ambrosoni; cuenta con un grupo de trabajo -está en el organigrama- dedicado a la gestión de seguridad de la información con integrantes de todo el Inciso; integra el Consejo Asesor Honorario de Seguridad de la Información -Cahsi- que funciona en Agesic; participa a pedido del Instituto Uruguayo de Normas Técnicas en el estudio de normas de gestión de seguridad de la información; capacita y genera conciencia a sus funcionarios en todo lo que tiene que ver con seguridad de la información mediante el continuo dictado de cursos.

A nivel del Consejo de Defensa Suramericano -del que formamos parte, y hoy tenemos la presidencia y la secretaría general- de la Unión Suramericana de Naciones, integra la red de apoyo ante incidentes cibernéticos -creada hace no mucho tiempo- entre los Ministerios de Defensa.

El centro de respuesta del Ministerio -Dcsirt- tiene los siguientes antecedentes. En setiembre de 2013 se firma un convenio con Agesic para el apoyo a nuestro Ministerio -por parte de Agesic- en la creación de un equipo de respuesta a incidentes cibernéticos. Luego de eso trabajamos bilateralmente con Agesic y también con el centro de respuesta nacional -Certuy-. En enero de este año se aprueba el Decreto 36/2015.

El Dcsirt es un equipo de respuesta a incidentes cibernéticos que trabaja en el ámbito del Ministerio, de manera alineada y colaborativa con el Certuy a nivel nacional y las redes de respuesta a incidentes cibernéticos que integran el MDN, como son el Cicte y el consejo de defensa. Las tareas principales del equipo son evitar incidentes, generar conciencia de seguridad y responder en caso de que se genere un incidente de seguridad cibernético para que el impacto sea el mínimo posible.

Existe un departamento de sistemas de información del Ministerio con un equipo dedicado exclusivamente a esta tarea. Actualmente se está extendiendo la gestión de seguridad de la información a todo el Inciso y promulgando una metodología única de gestión de incidentes en seguridad cibernética. Actualmente se evalúa la seguridad cibernética de estructuras críticas del Inciso y se ha dado participación al Certuy para la realización de estas tareas. Hay tareas que realizamos conjuntamente.

Tenemos una serie de misiones y tareas, entre ellas la de ser el centro coordinador de todas las tareas que tengan que ver con la prevención, atención y gestión de aprendizaje; contribuir al desarrollo técnico de especialistas; colaborar y coordinar actividades; concientizar y colaborar en el establecimiento de políticas de gestión de activos; colaborar en la difusión de implementación de las mejoras prácticas de seguridad, etcétera. Les dejamos esta información a la comisión.

Los objetivos trazados a corto plazo en seguridad en el Ministerio son: estandarizar la política de gestión de seguridad de la información en todo el Inciso; continuar participando en el ejercicio de seguridad, tanto a nivel nacional como internacional; capacitar en la conciencia de seguridad de la información de procedimientos ante incidentes y respuestas organizadas y colaborativas entre ellos; revisión y evaluación de los activos críticos del Inciso; y entrenamiento específico en caso de las estructuras críticas apoyados en el sistema de información particular.

Desde el punto de vista de una concepción militar, para nosotros existen cuatro niveles de actuación: político, estratégico, táctico y operacional. Desde el aspecto político nosotros actuamos a nivel de la cúpula del Ministerio, con responsabilidad, como se ha visto en el organigrama, en línea con lo que se determina a nivel nacional, a través de la Agesic. En el aspecto estratégico hemos determinado cierto tipo de niveles de actuación, de actividades y de esquemas que tienen que ver con realidades nacionales e internacionales. Para el aspecto táctico y operacional hemos creado el centro de respuesta, con un director y una estructura, y estamos trabajando en esta materia.

Hemos tomado como criterio y línea de acción que nuestro país y la región sufren una serie de amenazas. En base a ellas y a los activos tenemos que controlar cierto tipo de vulnerabilidades y los riesgos que pueden existir. Actuamos de manera activa y pasiva; en forma proactiva y reactiva, con respecto a los riesgos que se generan.

(Se suspende la toma de la versión taquigráfica)

SEÑOR PRESIDENTE.- Puede continuar el señor Subsecretario.

SEÑOR SUBSECRETARIO DE DEFENSA NACIONAL.- Queremos informar que según el índice de Cyber Seguridad Global, elaborado por la Unión Internacional de Telecomunicaciones, la UIT, organismo especializado de las Naciones Unidas para las

Tecnologías de la Información y la Comunicación, nuestro país -nos sentimos parte de ello como defensa- se encuentra segundo en América Latina y el Caribe, y octavo en el mundo.

La investigación que realiza la UIT, organismo de las Naciones Unidas, mide el nivel de desarrollo en el tema a partir del análisis de cinco categorías: medidas jurídicas, medidas técnicas, medidas de organización, capacitación y cooperación. Este es un dato interesante; a veces manejamos las cosas por la negativa y esta es una respuesta uruguaya, por la positiva.

Como conclusión de nuestra presentación -es lo que nosotros vemos como defensa; no quiere decir que sea la verdad global-, cabe señalar que nuestro país ya hace unos años que trabaja para adecuar su marco legal a los efectos de dotar al Estado de herramientas para el buen uso de las tecnologías de la información. Esto fue dispuesto por la Agesic, del CERTuy, DCSIRT entre otros, que procuran dar reglas claras de actuación en defensa de los derechos de los ciudadanos, de la protección de datos personales y del acceso a la información. Este esfuerzo queda de manifiesto en el posicionamiento alcanzado por Uruguay a nivel latinoamericano como en el contexto internacional según el índice que anteriormente mencioné.

La creación de la Agesic en el año 2007, el CERTuy y el DCSIRT en 2015 marcan el interés de regular los aspectos vinculados a la seguridad informática. Asimismo, se le otorga a esta agencia la facultad de apercibir y fiscalizar a los organismos que no cumplan con la normativa en vigencia.

Se constata un avance al establecer políticas de cyberseguridad comunes en las Unidades Ejecutoras 02 al 15 del Presupuesto Nacional.

Otro aspecto a destacar para nosotros es la existencia de procedimientos estandarizados para reportar los incidentes de seguridad que permitan determinar las violaciones a la seguridad. No obstante ello, aún no se puede evitar los efectos de los ataques que ponen a nuestro país en una situación de riesgo y de vulnerabilidad.

La creación del DCSIRT en el contexto del Ministerio de Defensa Nacional da cuenta del alcance estratégico con que se está manejando el tema. Otro aspecto que señala el riesgo en nuestro país en esta materia es no contar con la tipificación de los delitos informáticos. Creemos necesario -se está trabajando en ello- crear una ley sobre delitos informáticos. Cuando se presentan situaciones es necesario realizar interpretaciones de las leyes en vigencia y no de una ley específica, inexistente. Sin embargo, cuando los ataques provienen de otros países se hace más difícil aún tomar acciones legales.

Un aspecto no menor es que quienes utilizan los conocimientos informáticos para actuar al margen de la ley, se valen de todo tipo de medidas para acceder a los sistemas y no necesitan de recursos tecnológicos muy sofisticados para actuar, situación que hace mucho más difícil poder contrarrestar los efectos de los posibles ataques: *hackers*, grupos de acción con un objetivo común o Estados, que son los actores a los que a veces debemos enfrentarnos.

Como decíamos al principio: este es un terreno inmenso, no delimitado, al que todos estamos sometidos. Hoy todos quienes vivimos en este país estamos sometidos, a nivel virtual, a una situación que puede impactar notoriamente en todo lo que forma parte de la vida en sociedad de los uruguayos.

SEÑOR MAHÍA (José Carlos).- Antes que nada, quiero agradecer la presencia y la exposición del señor Subsecretario de Defensa Nacional. El tema de los delitos informáticos, como todos saben, está pendiente.

Al igual que el señor diputado Pablo González, integro la Comisión de Constitución, Códigos, Legislación General y Administración, donde se discutió la actualización del Código Penal, que ha tenido dificultades en otros aspectos, pues tiene más vinculación con la vida política cotidiana, concretamente a lo que refiere a los abusos de funciones. Todo aquel que haya pasado alguna vez por un cargo ejecutivo sabe que está presente lo dispuesto por ese artículo porque depende de la interpretación del Juez. Más allá de ello, existe interés en avanzar en esta materia. Habría que ver si esta propuesta se lleva adelante mediante una ley nueva o se incluye dentro de la modificación del Código Penal. Todos tenemos claro que al no haber aún en el Derecho Comparado un marco legal internacional ni convenciones acordadas que sean una referencia específica en un tema cuya naturaleza no solo es nacional sino también internacional, se hace difícil avanzar en la construcción de un nuevo marco legislativo.

Hace unos días leí que en Chile estaba la empresa *Kaspersky* reunida con gente especializada en programas antivirus y demás. Como se sabe, este grupo se encarga de señalar a los distintos *cyberataques* y anunció que en América Latina existe un potencial de riesgo, aunque no es la región del mundo en la que se pueda pensar como primer lugar de interés para los *ciberataques*. La referencia que hacía el señor subsecretario al ataque por el enriquecimiento de uranio tuvo que ver con Irán y con la relación de este país con Estados Unidos. Algo de similar naturaleza después se vio en la Casa de Gobierno de Francia.

En ese sentido, me gustaría conocer si hay algún tipo de cuidado o seguimiento en cuanto a la compra de ciertos paquetes vinculados a algunas empresas como, por ejemplo, *Cisco*, referidas a los vectores de seguridad. A través de algunas impresoras de determinadas empresas se puede conocer todo lo que nosotros imprimimos.

En tal sentido, me parece muy bueno el posicionamiento de Uruguay, la coordinación que se hace a nivel del Estado. A esta comisión concurrió la gente de la Agesic en un régimen muy similar tratando de trabajar con reserva en algunos aspectos comprometidos. Todos somos conscientes de que tarde o temprano estos hechos pueden darse y es importante es la capacidad de respuesta que podamos tener.

SEÑOR AMBROSONI (Roberto).- En cuanto a la pregunta formulada por el señor diputado Mahía sobre los aspectos técnicos, quiero señalar que coincido en un cien por ciento en que estamos en una época de transición técnica, inclusive a nivel social, y estamos cambiando conocimiento de todo esto por conciencia. Esto se puede observar desde el caso de los menores en Internet; todos tenemos esa transición. En el Consejo Asesor de Seguridad se está discutiendo ese tema para que esta información llegue a las escuelas y no haya más menores que se suiciden por *bullyng*, a nivel técnico es lo mismo y también es igual a nivel de los ministerios de defensa nacional. Lo que se aconseja es que todo el mundo trabaje en conjunto y que los equipos de respuesta interactúen.

Por otra parte, se mencionaba que existen algunos *softwares* cerrados o aplicaciones cerradas que tienen esas puertas cercenadas de conexión. Asimismo, se discute si a nivel de los sistemas operativos *Windows* esto también sucede. La realidad es que también estamos en la misma transición de discusión técnica porque, por ejemplo, para abatir este tema, se dice que deberíamos ir al *software* libre porque se supone que es abierto. También se discute que por más que sea abierto, ¿quién mira todo el código para darse cuenta de que no tiene ningún agujero o una puerta trasera? Esta discusión está arriba de la mesa en esta transición. Está muy discutido el tema de si utilizar el

software propietarios o *software* abierto porque por más que esté abierto y no se vea, es el mismo e igual está cerrado. Lo que todos estamos haciendo es un seguimiento técnico de los registros de vulnerabilidades y de los incidentes que se registran para tratar de estar al tanto lo máximo posible. Esta es una tarea bastante compleja porque todo esto a veces es muy nuevo, pues surgen *backdoors e incidentes* técnicos continuamente.

Ayer se descubrió a nivel de los sistemas operativos de los celulares un *backdoor*, aparentemente en los Galaxy S5, que hoy por hoy pululan en el mercado. Como que vamos siempre de atrás de todo esto. La realidad es que la discusión está arriba de la mesa y tratamos de ver por dónde va la cuestión. Una de las medidas ante los *software* cerrados, en el caso de activos críticos, es pedir el compromiso de que no existen puertas traseras o de que no se van a generar vulnerabilidades al respecto. En el caso de que exista, compartir la responsabilidad.

Uruguay de alguna manera se cubre con eso, con la ley de protección de datos personales que contempla el hecho de tercerizar datos, porque la norma exige que esos datos no queden expuestos. De alguna manera nuestro país está bastante cubierto pero las posibilidades de los agujeros están y los venimos siguiendo.

SEÑOR PRESIDENTE.- Sin lugar a dudas que este es un tema que da para muchísimo y en particular nos preocupa. Nosotros hemos trabajado fuerte en el tema de las tarjetas de crédito y este es un tema no menor en que a nivel de legislación Uruguay está muy descubierto, no solo con respecto a la protección de datos en lo legal sino también en relación a la realidad que todos manejamos, porque hay que ver hasta dónde van los derechos de cada uno. Pero, lamentablemente, no tenemos más tiempo y si el señor subsecretario está a disposición, sin ningún apuro, podemos seguir más considerando este asunto en otro momento.

Por otra parte, quisiéramos solicitar al señor subsecretario un informe, para cuando estime conveniente, sobre el tema misiones de paz y la visión del Ministerio de Defensa Nacional con respecto al Consejo de Seguridad, una realidad del Uruguay que nos cambiará a partir del 15 de octubre de este año. Ya queda oficialmente invitada esta delegación del ministerio que luego nos dirá en qué fecha puede concurrir.

SEÑOR CHIAZZARO (Roberto).- Nos gustaría que nos hicieran un informe sobre nuestra plataforma continental.

SEÑOR SUBSECRETARIO DE DEFENSA NACIONAL.- Tenemos buenas noticias en estos días. Nuestro ministerio participa en la comisión del Estado a través de ciertos representantes. De pronto cuando concurramos para considerar lo que refiere a las misiones, desde nuestro punto de vista podamos dar una pequeña información. Tampoco queremos abarcar lo que le compete al Ministerio de Relaciones Exteriores, que es el que preside esa comisión. Nosotros tenemos un equipo ahí, que estuvo en Nueva York hace unos días porque mantuvieron una reunión con la subcomisión correspondiente.

SEÑOR PRESIDENTE.- Entonces, ya comprometemos al señor subsecretario de Defensa Nacional por el tema de las misiones de paz, del Consejo de Seguridad en relación con estas misiones de paz, la plataforma continental y, de pronto, para hablar sobre algo más de este asunto de hoy.

Se levanta la reunión.

≠